Hoofdstuk Wifi-security

Inhoud

H1 WIFI

We gaan in dit hoofdstuk in op hoe het wifi-protocol in de basis werkt.

1. Inleiding

Het is 10 april 2018, als 4 russen van de geheime inlichten dienst van Rusland naar Nederland reizen. Het OPCW in Den Haag doet op dat moment onderzoek naar de moord op een Russische dubbel spion. Het vermoeden is dat Rusland deze man vergiftigd heeft, Rusland ontkent. Op 13 april worden deze 4 russen opgepakt, in een auto op een parkeerterrein naast het OPCW. In de auto appratuur om wifi te hacken, wat waren ze van plan?

Opdracht 1. Wifi hacken in het nieuws

In het onderstaande filmpje krijg je informatie over een mogelijke hack operatie van de Russische inlichtingen dienst in Nederland. Ze wilde informatie krijgen door het wifi netwerk te hacken.

1. Bekijk het filmpje op YouTube.

https://www.youtube.com/watch?v=xq0DjrpMt4s

Het is overal om heen eens, in de trein, in een restaurant, een supermarkt, de sportvereniging, je school, thuis etc. Het gaat hier over wifi. Het **protocol** van wifi is ontworpen door de Wifi Alliance in 1997 en sindsdien kunnen we er bijna niet meer om heen. In 2018 waren er naar schatting 22 miljard wifi-apparaten actief over de gehele wereld. Dit zijn apparaten van je telefoon en laptop tot een mediacast, printer en camera's. In dit hoofdstuk gaan we in op wat wifi is en hoe het is beveiligd.

Opdracht 2. Wifi is overal

2. Doe de volgende quiz met de hele klas als aftrap van het onderwerp.

Leerdoelen

Dit zijn de leerdoelen voor dit hoofdstuk:

Leerdoel	**Ik kan dit nog niet**	**Ik kan dit een beetje**	**Ik kan dit**
Je kunt in hoofdlijnen de stappen van het wifi protocol van een open netwerk beschrijven en toelichten.			
Je kunt het verschil benoemen tussen de verschillende modulaties van de zes wifi-versies.			

Je kunt van de wifi-netwerken om je heen uitzoeken welke modulatie, versie en kanaal deze netwerken zitten.			
Je weet het verschil tussen een open en gesloten netwerk.			
Je kunt een mogelijke aanval op een wifi-netwerk herkennen en uitleggen (wireless hijacking).			
Je kunt maatregelen benoemen en toelichten ter bescherming tegen wireless hijacking.			
Je kunt uitleggen in hoeverre het filteren op MAC-adressen geschikt is om de toegang tot een wifi-netwerk te beveiligen.			
Je kunt in hoofdlijnen de verschillen benoemen tussen WEP, WPA en WPA2, protocollen voor versleuteling van gegevens via een wifi-netwerk.			

Begrippen

Dit zijn de belangrijkste begrippen, het is belangrijk dat je deze begrippen goed kent.

Wifi Protocol	Protocol voor het draadloos verbinden van apparaten. Het protocol wordt ook wel het 802.11 protocol genoemd.
Open netwerk	Een wifi-netwerk waar je geen wachtwoord hoeft in te vullen om te verbinden. De berichten die worden verstuurd zijn niet versleuteld.
Gesloten netwerk	Een wifi-netwerk waar je wel een wachtwoord moet invullen om te verbinden. De berichten zijn wel versleuteld.
Wireless Access Point (WAP)	Toegangspunt voor het verbinden via een draadloos netwerk.
SSID	Service Set Identifier, de naam van een wifi netwerk waarmee een router zichzelf kenbaar maakt.
Wireless Hijacking	Een aanval waarbij iemand een wifi-netwerk imiteert.
MAC-adres	Uniek adres dat iedere netwerk-module heeft.
Spoofen	Het aanpassen van waardes, bijvoorbeeld het aanpassen van het MAC-adres.
MAC-adresfilter	Het filteren van MAC-adressen om juist wel (white-list) of juist niet (black-list) te laten verbinden.

WEP	Eerste vorm van versleuteling van gegevens over een wifi-netwerk, inmiddels eenvoudig te kraken.
WPA	Verbeterd protocol voor versleuteling van gegevens over een wifi-netwerk, maar inmiddels ook niet veilig meer.
WPA2	Verbeterde versie van het WPA-protocol.

2. Wifi-versies

Wifi is de afkorting voor 'Wireless Fidelity', wat zoiets betekent als: draadloze betrouwbaarheid. Het wifi-protocol is een standaard over hoe apparaten draadloos met elkaar communiceren. Het bestaat dus uit een aantal vaste afspraken. Het wifi-protocol werd bedacht in 1997. Op dit moment kennen we nog steeds hetzelfde wifi protocol, beter bekend als 802.11. Door de jaren heen is daar wel een aantal nieuwe modulatietechnieken (ook wel versies genoemd) bijgekomen, deze zijn herkenbaar aan de letters achter de naam. Er zijn 6 verschillende versies gemaakt, al deze versies hebben hun eigen naam en eigen kenmerken. Zo verschilt per versie de snelheid en het theoretisch bereik van het wifi-netwerk. Een overzicht van de verschillende versies met eigenschappen kan je vinden in Tabel 1.

802.11 Protocol met modulatie letter	Wifi Versie	Uitgebracht	Frequentie(Ghz)	Bruto Snelheid (Mbps)	Netto snelheid (Mbps)	Bereik binnenshuis (in meters)	Bereik buitenshuis (in meters)
-		1997	2.4			20	100
a	(Wifi 2)	September 1999	5	54	25	35	120
b	(Wifi 1)	September 1999	2.4	11	5	38	140
g	(Wifi 3)	Juni 2003	2.4	54	25	38	140
n	Wifi 4	Oktober 2009	2.4	150 tot 600	65 tot 250	70	250
n	Wifi 4	Oktober 2009	5	450 tot 1800	200 tot 800	50	140
ac	Wifi 5	2014	5	433 tot 2600	200 tot 1200	70	250
ax	Wifi 6	2018	5	1148 tot 4800	450 tot 2200		

TABEL 1 OVERZICHT VAN WIFI-VERSIES.

In de eerste kolom staan de letters die achter het protocol zijn toegevoegd, zodat we duidelijkheid scheppen in de communicatie. Je praat dus bijvoorbeeld over een 802.11n protocol, dat noemen we dan ook wel Wifi 4. Verder zie je in de tabel de bruto en netto snelheid. De bruto snelheid is de theoretisch snelheid die mogelijk is als de verbinding maar één richting in zou worden gebruikt. In praktijk gebruik je het echter in twee richtingen, waardoor de bandbreedte verdeeld moet worden. De netto snelheid is daarom de maximum snelheid die je kunt ervaren als je op wifi zit. In de laatste twee kolommen zie je het mogelijke bereik van wifi. In praktijk is dit sterk afhankelijk van de aanwezigheid van andere wifi-apparaten en fysieke obstakels. Verder bevat de tabel een kolom met de frequentie waarover wordt uitgezonden. Tot nu toe gebruiken we 2.4 GHz en 5.0 GHz.

Opdracht 3. Overzicht van wifi-versies

Bestudeer Tabel 1 en beantwoord de volgende vragen?

3. Wat is het verschil in bereik(zowel binnen als buitenhuis) tussen 2.4 GHz en 5.0 GHz? En wat is het verschil in snelheid tussen 2.4 GHz en 5.0 GHz?
4. Welk wifi-protocol heeft de hoogste snelheid?
5. Welke wifi-versie heeft twee verschillende frequenties ?

Routers en wireless access-points

Om te verbinden met een netwerk moet je in de buurt zijn van een wireless acces point (WAP). Een WAP is als een netwerkkabel die je in je computer stopt om verbinding te maken met het netwerk. De kabel is alleen vervangen door een draadloze verbinding.

Een router heeft als functie om netwerken aan elkaar te koppelen. Waarschijnlijk heb je thuis een router die je thuisnetwerk koppelt aan het internet. Een router is vaak ook een access-point, vooral de routers die in thuisnetwerken worden gebruikt.

Opdracht 4. Een wifi-router kopen

In Figuur 1.2 zie je een doos waar een wifi router in zit als die verkocht wordt. Deze doos bevat de informatie in termen van wifi netwerken. Bekijk de figuur goed en beantwoord de volgende vragen met behulp van Tabel 1.

FIGUUR 1.1 DOOS VAN EEN WIFI-ROUTER

6. Welke wifi-protocol gebruikt deze router? Waar zie je dat?
7. Als de router binnenshuis staat, en ik sta op 30 meter afstand van de router. Kan ik dat verbinden met de router?

Bij sommige routers, zoals deze, kun je de antennes zien, bij andere routers zijn ze verwerkt in het apparaat. Door de antennes anders te richten (bijvoorbeeld horizontaal en verticaal) kan het bereik van de router worden verbeterd.

Je kunt niet direct zien welke versie van wifi je gebruikt op je telefoon. De Wifi Alliance wil dat in de toekomst telefoons en computers laten zien met welke versie wifi je bent verbonden. Je zult dan bijvoorbeeld op je telefoonscherm een klein cijfer bij je wifi symbool zien. Zie Figuur 1.1 voor hoe dat eruit gaat zien later.

FIGUUR 1.2 SYMBOLEN BIJ WIFI-VERSIES

Je kunt er met een app echter wel achter komen welke wifi-versie je gebruikt. In de google Play store (voor Android telefoons) heb je bijvoorbeeld: Wifi Analyzer. In de Apple store heb je bijvoorbeeld: Network analyzer. Verder bestaat er ook software

voor computers die dit kunnen, deze kun je vinden via google. Zoek maar eens op ‘wifi analyzer’ of ‘network analyzer’.

Opdracht 5. Welke netwerken zijn er om je heen?

Download de juiste app voor je mobiele telefoon en achterhaal de volgende informatie:

- Naam van het netwerk
- Op welke frequentie communiceert het netwerk (2.4 GHz of 5.0 Ghz)
- Welk kanaal gebruikt het netwerk? Een wifi-netwerk maakt gebruik van een bepaald kanaal. Voor wifi op 2.4 GHz zijn er 14 kanalen.
- De wifi-versie

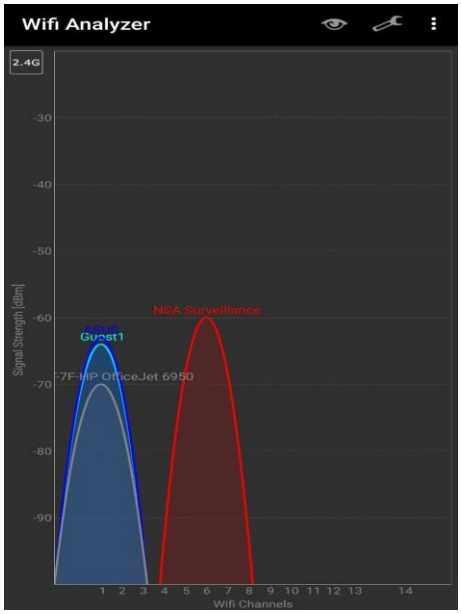
8. Schrijf de resultaten van je onderzoek op in de onderstaande tabel.

Naam netwerk	Frequentie (Ghz)	Kanaal	Wifi Versie

TABEL 2 WIFI-VERSIES VAN NETWERKEN OM JE HEEN

Voorbeeld wifi analyzer Android:

Zorg dat de app toegang heeft tot je locatie, anders werkt de app niet. Als je de app opent zou iets moeten zien dat lijkt op Figuur 1.3. Hier zie je op y-as de signaal sterkte en op de x-as de wifi-kanalen. Het wifi-netwerk ‘NSA surveillance’ zit op kanaal 6 (daar zit de hoogste piek) en straalt uit richting kanaal 4 en 8.



FIGUUR 1.3 WIFI-ANALYZER

Klik op het oogje rechtsboven en selecteer AP List. In het overzicht dat je nu krijgt is de bovenste het wifi netwerk waarmee je nu verbonden bent. Druk hierop en bekijk de linkspeed, nu kan je erachter komen welke wifi versie je gebruikt met behulp van Tabel 1. Later ga je de app nog nodig hebben, dus verwijder hem niet gelijk!

Open en gesloten netwerken

We maken in deze module onderscheid tussen 2 verschillende wifi netwerken.

- Een **open wifi netwerk**. Dit is een netwerk waar geen wachtwoord hoeft worden ingevuld om te verbinden. Als je in de buurt bent kan je dus altijd verbinden en gelijk internetten. Belangrijk is dat bij dit type wifi netwerken **GEEN** versleuteling van berichten plaatsvind tussen WAP en het verbonden apparaat (bijvoorbeeld je mobiele telefoon).
- Een **gesloten wifi netwerk**. Dit is een netwerk waar je wel een wachtwoord moet invullen om te verbinden. Een gesloten wifi netwerk maakt **WEL** gebruik van een versleuteling bij het versturen van berichten tussen apparaat en WAP.

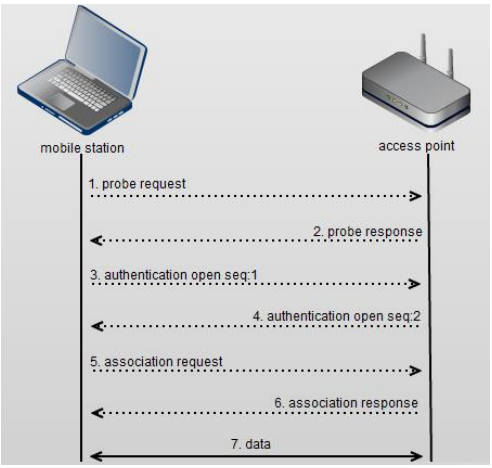
Het is belangrijk om te beseffen dat alle berichten die worden uitgewisseld tussen een WAP en een ander apparaat afgeluisterd kunnen door een hacker die in de buurt van het netwerk is.

Opdracht 6. Aanvallen op wifi-netwerken?

9. Noem een mogelijke aanval van een hacker op een open wifi-netwerk?
10. Noem een mogelijke aanval van een hacker op een gesloten wifi netwerk?

3. Protocol bij een open netwerk

Om te verbinden met een WAP voor een **open netwerk** wordt het 802.11 protocol gebruikt. Een visualisatie van dit protocol zie je in Figuur 1.4[1]. Rechts zie je een WAP, links zie je een apparaat (laptop, telefoon, etc) dat verbinding wil maken met het WAP.



FIGUUR 1.4 WIFI-PROTOCOL

- Het apparaat stuurt een *probe request* (bericht 1) met daarin onder meer informatie over de wifi-versies die het apparaat ondersteunt. Alle WAP's in de buurt ontvangen dit bericht en kunnen reageren met een *probe response* (bericht 2). In dit bericht staat onder meer het **SSID** (Service Set Identifier) van het draadloze netwerk.

Deze eerst twee berichten kan je zien als het zoeken naar wifi-netwerken vanuit een telefoon. Op je telefoon gebeurt dit met regelmaat zodat je een lijstje kunt zien met beschikbare netwerken.

- In bericht 3 en 4 vind er **authenticatie** plaats, beide apparaten maken zich kenbaar met hun MAC-adressen.

Ieder apparaat heeft een uniek MAC-adres. Het MAC-adres is 48 bits lang en wordt meestal in hexadecimale vorm aangeduid, bijvoorbeeld 00:0C:6E:D2:11:E6.[2] Er is geen beveiliging op de authenticatie. In principe wordt ieder apparaat geaccepteerd, tenzij het WAP alleen bepaalde MAC-adressen toelaat.

- Met bericht 5 *(association request)* laat het apparaat zien dat het een verbinding wil maken. De meeste WAP's houden een unieke ID voor ieder apparaat dat is verbonden. De WAP reageert met bericht 6 (*association response)* waarmee de verbinding is opgezet.

Nu is het apparaat verbonden met het netwerk en kan data worden uitgewisseld (stap 7).

[1] Bron: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_Process_Explained
[2] Bron: https://nl.wikipedia.org/wiki/MAC-adres

Opdracht 7. Het wifi-protocol 802.11

Een apparaat wil verbinden met een wifi-netwerk. Voor het beantwoorden van onderstaande kun je gebruik maken van Figuur 1.4.

11. De volgende acties worden uitgevoerd:

Apparaat		WAP
Probe request	→	
	←	Probe response

    Welk bericht gaat het apparaat nu versturen?

12. De volgende acties worden uitgevoerd:

Apparaat		WAP
Probe request	→	
	←	Probe response
Authentication request	→	

    Hoeveel berichten worden er nog heen en weer gestuurd voordat er data wordt verstuurd?

13. De volgende acties worden uitgevoerd:

Apparaat		WAP
Probe request	→	
	←	Probe response
Authentication request	→	

    Nu komt het apparaat buiten het bereik van de WAP. Vervolgens is het bereik terug. Wat is het volgende bericht dat wordt verstuurd?

14. De volgende acties worden uitgevoerd:

Apparaat		WAP
Probe request	→	
	←	Probe response
Authentication request	→	
	←	Authentication response
Association request	→	
	←	Association response

    Kan het apparaat nu data versturen via het WAP?

Vervolg

We kijken in het vervolg van deze module naar de volgende drie onderwerpen:

- **Authenticatie van de WAP**: hoe weet je zeker dat je met de juiste WAP te maken hebt?
- **Authenticatie van de gebruiker**: hoe weet de WAP zeker met een gebruiker te maken te hebben die toegang mag krijgen
- **Versleuteling van de gegevens** tussen gebruiker en WAP

4. Authenticatie van WAP

In dit hoofdstuk leer je wat de russen uit het filmpje in de inleiding van dit hoofdstuk precies van plan waren.

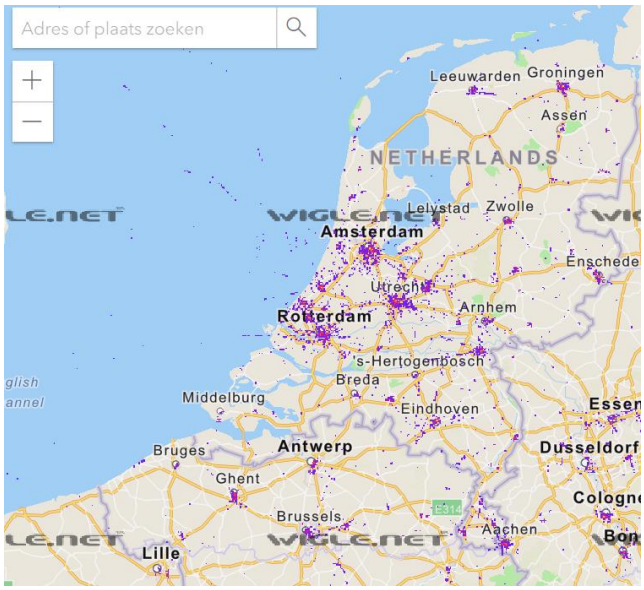
Iedere wifi netwerk om je heen is op een manier uniek. Ze zenden namelijk allemaal een SSID (Service Set Identifier) uit in het probe response (zie vorige hoofdstuk). Wat erg interessant is van deze SSID, is dat het vaak informatie bij zich draagt van het bedrijf. Denk aan Starbucks wifi, Wifi in de Trein, Airport wifi. Een wifi-netwerk maakt zichzelf kenbaar door middel van dit SSID.

Opdracht 8. Verken SSID wereldwijd

Er is een website die alle locaties van SSID in kaart heeft gebruikt, daarmee kan je veel wifi netwerken verkennen.

Ga naar www.wigle.net, daar kun je rechts bij SSID de naam van een wifi netwerk invullen en door onder in dat blok op filter te drukken laat de website zien waar deze wifi netwerken zijn. Ieder paars puntje is een wifi netwerk. Let wel op! De SSID die je intypt is hoofdletter gevoelig, zorg dus dat je het goed intypt. Voer de volgende opdrachten uit en beantwoord de vragen

15. Zorg dat je de hele wereld ziet en filter op niks. Wat zie je nu hier, en wat betekent het geel en paars wat je ziet? Waar zijn de meeste wifi netwerken?
16. Zorg dat je de kaart van Nederland ziet, en filter de website dan op: Eduroam. Eduroam is de naam voor alle wifi's op universiteiten en hogescholen in heel Europa! Zoom in op de stad waar jij graag wilt studeren en zoek uit waar jouw hogeschool/universiteit zit.



FIGUUR 1.5 WIFI-PROTOCOL

17. Zorg dat je de kaart van het dorp/stad ziet waar je school is. Filter de website op het netwerk naam van je school. Kan jij je eigen school vinden?
18. Onderzoek of jij je eigen wifi-netwerk thuis kan vinden. Leg uit hoe je dit hebt aangepakt. (Het kan zijn dat je hem niet kan vinden, deze website heeft nog niet alles, als je wifi netwerk redelijk nieuw is zal het nog niet zichtbaar zijn)
19. Zorg dat je de kaart van Nederland ziet. Zoek uit hoe het wifi netwerk van McDonalds heet en filter dit op de website, zie jij waar alle vestigingen zitten? Maak hiervan een foto

Opdracht 9. Wifi-netwerk hacken

Voordat je het filmpje over het hacken van een wifi-netwerk gaat bekijken, geef antwoord op de volgende vraag.

20. Met de kennis over SSID's, wat zou een hacker kunnen doen om via een wifi-netwerk iemand af te luisteren?

In onderstaand artikel zie je Sanne, zij is ethisch hacker en kan informatie verkrijgen via wifi-netwerken. Bekijk onderstaand filmpje en beantwoord de vragen.

https://www.nu.nl/243360/video/zo-breken-hackers-in-op-een-openbaar-wifi-netwerk.html

21. Welke data kunnen hackers allemaal verkrijgen volgens Sanne?
22. Op welke manier krijgt Sanne het wifi wachtwoord van de interviewer? Leg uit wat ze gedaan heeft
23. Wat moet je volgens het filmpje doen om te zorgen dat dit niet bij jou gebeurt?
24. De journalist had kunnen weten dat het om een nep website ging? Heb je gezien hoe hij dat had kunnen weten?

Wireless hijacking

Je hebt kunnen zien dat het niet veilig is om verbinding te maken met willekeurige netwerken:

- **Open netwerken**, waar je geen wachtwoord voor nodig hebt, kunnen eenvoudig worden afgeluisterd.
- Maar ook **gesloten netwerken** zijn niet veilig. In het filmpje uit de vorige opdracht wordt duidelijk dat je met een wifi Pineapple eenvoudig een wifi-netwerk kunt maken.
    - Bij **openbare netwerken** (netwerken bij cafe's, restaurants, etc) kun je met de Pineapple zorgen dat telefoons verbinding maken zodat je mee kunt luisteren.
    - Zelfs bij niet-openbare netwerken is een aanval met zo'n apparaat mogelijk.

FIGUUR 1.6 WIFI PINEAPPLE

Het 'lokken' van apparaten en mensen om verbinding te maken met jouw wifi-netwerk heet ook wel wireless hijacking. In Nederland is dit beter bekend als de 'Wifi in de trein aanval'.

De russen uit het filmpje in de inleiding van dit hoofdstuk hebben dat geprobeerd: wireless hijacking. Ze hadden een wifi Pineapple in de auto liggen. Waarschijnlijk probeerden ze te zorgen dat telefoons en laptops van medewerkers van het OPCW verbinding zouden maken met hun wifi-netwerk om op die manier vertrouwelijke gegevens te verkrijgen.

Eigenlijk kun je je hier nauwelijks tegen beschermen. Een telefoon zendt namelijk regelmatig een bericht uit (probe request) met daarin de lijst van opgeslagen SSID's. Een Pineapple kan dit lezen en vervolgens een netwerk met zo'n SSID opzetten. De telefoon maakt verbinding en stuurt het wachtwoord van het netwerk naar de PineApple.

Opdracht 10. Wireless hijacking met een klasgenoot

Het doel van deze opdracht is om met een klasgenoot een keer wireless hijacking te proberen. Je hebt hiervoor 2 telefoons nodig waarbij een van de twee een hotspot kan starten. Belangrijk voor je begint:

25. Bespreek met je klasgenoot wat er gaat gebeuren. Je zal geen data van hem stelen en tegen hem gebruiken. Je zult ook geen pakket vanger zoals wireshark aan hebben staan.

In dit experiment zal een telefoon dienen als WAP door middel van de hotspot functie, de andere telefoon zal het slachtoffer zijn en een verbinding maken met de WAP.

26. Doorloop de volgende stappen

Hacker telefoon:

- Je telefoon moet een open hotspot kunnen aanmaken. Dat kan met Android, bij Apple gaat dat niet.
- Vraag of het slachtoffer een SSID van een open netwerk (dus zonder netwerk) heeft opgeslagen in de telefoon. Gebruik dit SSID. Als hij/zij geen open netwerk heeft, laat hem/haar er dan eentje aanmaken.
- Ga naar je instellingen van je telefoon en start een hotspot op met het SSID, zonder wachtwoord.
- Start de hotspot en klaar ben je, laat nu het wifi protocol zijn werk doen.

Telefoon van slachtoffer:

- Zorg dat het vinkje automatisch verbinden op aan staat voor wifi en het open netwerk.
- De telefoon mag niet verbonden zijn met een ander wifi netwerk

Als bovenstaande stappen juist zijn uitgevoerd zal de telefoon van de slachtoffer automatisch verbinden met de hotspot van de hacker. Vanaf dat moment zal alle data via de telefoon van de hacker gaan. Als dit gelukt is draai je de rollen om.

Let op: Mocht je een gesloten netwerk willen gebruiken, dan moet je of zelf een identiek wachtwoord aan je eigen hotspot toevoegen. Of een willekeurig wachtwoord maar dan zal de telefoon van de slachtoffer niet verbinden (wel proberen).

Bescherming tegen wireless hijacking

Hierboven zag je hoe makkelijk het kan zijn om deze aanval uit te voeren. Nu is het belangrijk dat dit niet bij jou gebeurd, of mensen om je heen. Je kunt je hier tegen beveiligen.

- **Zet wifi uit als je het niet gebruikt**

Het klinkt misschien heel logisch, maar toch doet bijna niemand het. Zet je wifi uit als je het niet gebruikt, op deze manier kan je niet per ongeluk verbinden met een hacker.

- **Ga alleen op wifi dat je vertrouwt, en gebruik anders 4G**

Hackers kunnen dus ook neppe hotspots starten met namen die jij denkt te vertrouwen. Gebruik dus alleen wifi van plekken die je vertrouwt. Dat zijn plekken zoals thuis en op school of bij vrienden. Gebruik geen wifi midden in het centrum van een stad met een naam die overkomt alsof ze(een hacker) wil dat je hem gebruikt.

- **Gebruik HTTPS**

Als jij op een website zit die HTTPS heeft, kan een hacker misschien wil je berichten lezen, maar hij kan ze niet ontcijferen. De sleutel die je gebruikt voor de HTTPS is namelijk al eerder uitgewisseld en de hacker zal alleen versleutelde berichten krijgen.

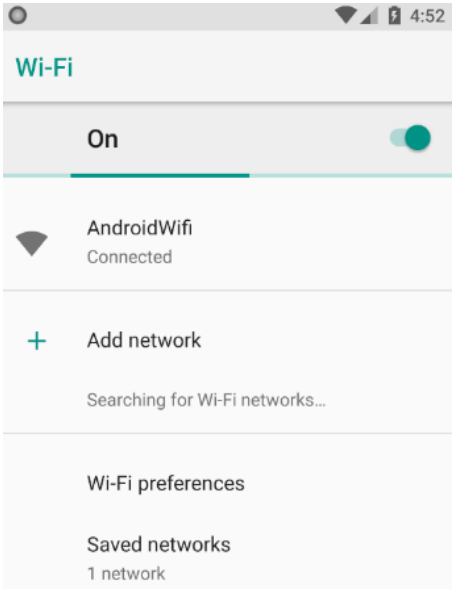
Als je browser of app een melding geeft dat de website niet wordt vertrouwd, open de website dan niet en voer vooral geen wachtwoord in. Controleer ook of je de juiste URL hebt.

- **Gebruik een VPN**

Mocht je zeker willen weten dat een hacker geen bericht kan lezen dat tussen jou en de WAP verstuurd wordt, gebruik dan een VPN! Dit versleutelt namelijk automatisch alle berichten die je telefoon verlaten.

- **Hou de lijst van opgeslagen netwerken schoon**

In je telefoon worden de netwerken waarmee je verbonden was opgeslagen, daar ligt een deel van het probleem. Door in deze lijst alleen netwerken te hebben die je echt vertrouwd maak je de kans al kleiner dat je ooit wordt aangevallen. Als je dus ooit met een open wifi netwerk verbindt (Free Wi-Fi) zorg dan dus dat je gelijk dit netwerk weer vergeet als je klaar bent met internetten. Hieronder staat hoe je dat kunt doen.



FIGUUR 1.7 GEEN OPGESLAGEN NETWERKEN

Android: Bij Android telefoons kun je naar je wifi-instellingen gaan, daar heb je vaak een optie in de trend van opgeslagen netwerken (Saved Networks, zie Figuur 1.6). Klik daar op en verwijder, door middel van vergeten, bij de wifi netwerken waar je ooit eenmalig mee verbonden bent geweest en daarna nooit meer gebruikt hebt. Ook wifi netwerken die een veel voorkomende naam hebben kan je beter verwijderen. Let op, als je een wifi netwerk vergeet gaat het opgeslagen wachtwoord ook verloren. Mocht je het wachtwoord niet meer weten of verbind je vaak met dit netwerk, dan kan je hem er beter in laten staan.

Apple: Bij Apple telefoons is dit helaas wat moeilijker. Je kunt deze lijst die Android heeft niet zien. Je zou je volledige *Netwerk instellingen* kunnen resetten. Hiermee verwijder je alle wifi netwerken die opgeslagen zijn, dan ben je in een keer klaar maar misschien minder praktisch want daarna moet je thuis, op school, etc. alle wachtwoorden opnieuw invullen. Je kan hier wel een netwerk verwijderen als het wifi netwerk binnen bereik is. Dat doe je door op de i te drukken naast de wifi naam en dan op “vergeet dit netwerk” te drukken. Dus mocht je binnenkort weer eens in de buurt zijn van een Free Wifi zorg dan dat je hem gelijk verwijderd.

Bovengenoemde stappen kunnen ook op een computer, in de praktijk is het aantal wifi wachtwoorden daar wat minder omdat ze vooral thuis worden gebruikt. Controleer dit als je thuis bent!

Opdracht 11. Wifi beveiligen

27. Open je telefoon en maak de lijst van opgeslagen netwerken schoon.

Beantwoord nu onderstaande vragen samen met een klasgenoot.

28. Hoeveel open netwerken had je (netwerken zonder wachtwoord)?
29. Hoeveel wifi-netwerken heb je verwijderd die je niet meer gebruikte?
30. Welke wifi-netwerken hadden jij en je buurman allebei staan die je hebt verwijderd?
31. Het uitzetten van wifi is vaak geen gewoonte bij mensen als ze uit huis gaan. Ga jij dit doen?

Opdracht 12. Authenticatie van het WAP

Je weet nu dat de enige authenticatie van het WAP plaatsvindt via het SSID. En je hebt gezien dat dat SSID heel makkelijk is na te bootsen.

32. Toch zou het wel mogelijk moeten zijn om een veilige authenticatie van een WAP te creëren. Wat zou je kunnen doen? Tip: denk aan hoofdstuk 6 van deze module.

5. Authenticatie van gebruiker en apparaat

In de vorige deel zagen we dat er nauwelijks authenticatie van de WAP plaatsvindt. Het is voor een apparaat moeilijk om te bepalen of de WAP waar het mee communiceert niet van een hacker is. Hoe is dat andersom? Hoe wordt het apparaat geauthentiseerd? En kun je daarmee voorkomen dat een hacker verbinding maakt met het wifi-netwerk?

Een apparaat identificeert zichzelf bij een WAP door middel van een **MAC-adres.** Een MAC adres wordt vaak weergeven als een fysiek adres (Physical Adres) en zou er als volgt uit kunnen zien: 00:1A:C2:7B:00:47. Het zijn 6 getallen tussen de 0 en 255, weergegeven in hexadecimale waarde. Iedere apparaat dat met een netwerk kan verbinden heeft een MAC-adres, of zelfs meerdere. Dat betekent dat als je laptop met internet kan verbinden via wifi en via een netwerkkabel, de laptop 2 verschillende MAC adressen heeft.

Het gebruik van wachtwoorden is natuurlijk ook mogelijk, daar komen we later op terug.

Opdracht 13. Wat is het MAC-adres van mijn apparaat?

In deze opdracht ga je onderzoeken wat het MAC adres is van je eigen computer of telefoon. Het verschilt per apparaat hoe je dat moet achterhalen. Hieronder staan de stappen uitgewerkt.

33. Probeer het MAC-adres te achterhalen van jouw apparaat, bijvoorbeeld van je telefoon. Het kunnen er zelfs meerdere zijn. Gebruik onderstaande tabellen daarvoor of zoek zelf op internet hoe je het MAC-adres kunt achterhalen.

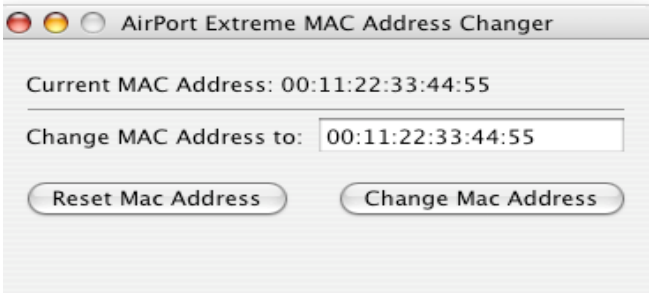
Besturingssysteem	**Windows 10, 8, 7 en Vista:**	**Linux / Unix**	**Macintosh OS X**
Stap 1	druk op ⊞+r	Zoek bij programma's naar terminal en klik hierop	Druk op Apple icon (linksboven) > System preferences > Network > Advanced
Reactie	Er opent zich een venster met als titel uitvoeren	Een terminal opent zich	Een scherm opent zich
Stap 2	Typ daar: "cmd" en druk op enter. (Het is mogelijk dat dit op school geblokkeerd is, voer het dan uit op je telefoon)	Typ ifconfig	Selecteer wifi
Reactie	Een terminal opent zich op je computer, herkenbaar aan de zwarte achtergrond	XXXXX	XXXXX
Stap 3	Typ daar: ipconfig /all (let op de spatie tussen ipconfig en /)	XXXXX	XXXXX
Reactie	Alle apparaten in je computer die met internet kunnen verbinden worden nu weergeven. Hier staat je MAC adres achter physical adres.	Alle apparaten in je computer die met internet kunnen verbinden worden nu weergeven. Hier staat je MAC adres achter physical adres.	A Wi-Fi Address or Airport Address displays. This is your device's MAC address.
MAC Adres:			

Besturingssysteem	**IOS**	**Android**	**Chromebook**
Stap 1	Setting > General > About	Settings > About Device > Status.	Click the status area, where your account picture appears.
reactie	Er opent zich een venster met als titel uitvoeren		
Stap 2			Click the section that says Connected to and the name of your network.
Reactie	XXXXX	XXXXX	
Stap 3	XXXXX	XXXXX	At the top of the box that appears, pick your network
Reactie	A Wi-Fi Address displays. This is your device's MAC address.	A Wi-Fi Address or WiFi MAC Address displays. This is your device's MAC address.	In the window that opens, the MAC address is the Hardware address.
MAC Adres:			

Een WAP kan apparaten toestaan en weigeren om verbinding te maken met het network op basis van een lijst met MAC-adressen. Dit wordt ook wel **MAC-adresfilter** genoemd. Je kunt een lijst maken met MAC-adressen die geen toegang mogen krijgen (een black-list). Je zou kunt ook een lijst maken met MAC-adressen die juist wel mogen verbinden (een white-list).

Wat kan een hacker nu doen om toch toegang te krijgen?

1. De hacker moet eerst een MAC-adres achterhalen dat op de white-list staat van de WAP. Dat is niet zo moeilijk. Bij het opzetten van een verbinding stuurt een apparaat immers het MAC-adres in bericht 3 (authenticatie), zie Protocol bij een open netwerk. Die berichten zijn niet versleuteld en dus makkelijk af te luisteren.
2. Als de hacker eenmaal in bezit is van het MAC-adres is het een koud kunstje om het MAC-adres te **spoofen**. Spoofen is het aanpassen van waardes waardoor de WAP niet het echte MAC-adres ontvangt (zie Figuur 1.8).



FIGUUR 1.8 MAC-ADRES SPOOFEN

Opdracht 14. SPOOF je MAC-adres

In deze opdracht ga jij je eigen MAC-adres spoofen.

34. Zoek hieronder in de tabel het juiste besturingssysteem en klik op de link. Daar staat uitgelegd hoe je het MAC-adres kan spoofen. Probeer dit uit.

Besturingssysteem	**Website**
Windows 10, 8, 7 en Vista:	https://www.groovypost.com/howto/change-mac-address-windows-10-why/
Linux / Unix	https://wiki.archlinux.org/index.php/MAC_address_spoofing
Macintosh OS X	https://blog.macsales.com/43777-tech-101-spoofing-a-mac-address-in-macos-high-sierra/
Chromebook	https://www.techjunkie.com/change-mac-address-chromebook/
Android	https://www.droidviews.com/change-mac-address-android-devices/
IOS	Niet mogelijk

Gratis wifi?

Ben je ooit in een hotel geweest waar je moest betalen voor de wifi? Of dat je ouders een account hadden gekocht en dat het daarna niet bleek te werken op jouw telefoon omdat je maar 1 apparaat mocht gebruiken met de gebruikersnaam en wachtwoord die je ouders kregen toen ze het account kochten. Of wat denk je van de gratis wifi op een vliegveld voor een half uur (zie Figuur 1.9).

FIGUUR 1.9 GRATIS WIFI VOOR 30 MINUTEN

Beide systemen werken op dezelfde manier. De WAP houdt een lijst bij van de MAC-adressen van apparaten die verbonden zijn. Mocht je op zo een plek zijn en je eigen MAC-adres spoofen, dan gaat er een wereld voor je open. Op een luchthaven kan je het MAC-adres aanpassen naar een willekeurig adres, de WAP herkent je als nieuwe gebruiker en je kan weer een half uur op het internet. In een hotel moet je het MAC-adres aanpassen naar een apparaat die op dat moment al toegang heeft.

Spoofen van je MAC-adres is niet illegaal, het gebruiken om geen geld te betalen voor de wifi wel.

Je dit als eigenaar tegengaan door met een ticketsysteem te werken. Dat zie je wel eens in koffietentjes. Op de kassabon staat een code, waarmee je voor een half uur toegang krijgt. De WAP koppelt die code aan het MAC-adres dat je gebruikt. Het spoofen van het MAC-adres heeft dan geen zin.

Opdracht 15. Spoofing

Geef antwoord op de volgende vragen

35. In een hotel moet je betalen voor wifi, de apparaten die mogen verbinden worden bijgehouden door een white-list in de WAP. Een hacker maakt gebruik van MAC-adres spoofing, en gebruikt een MAC adres uit de white-list. Zou je dan kunnen verbinden?
36. Op het vliegveld werkt de WAP met een white list, als je wilt verbinden moet jij je eigen email adres opgeven want daar komt een code op binnen die je moet invullen tijdens het aanmelden. Na een half uur wordt je

verbinding verbroken en wil je opnieuw verbinden, hoe zou je nu opnieuw kunnen verbinden zonder dat de WAP ziet dat je voor een 2de keer verbinding maakt?

37. Een hoteleigenaar heeft een ticketsysteem voor zijn wifi. Hij kiest ervoor om alle MAC-adressen die er bestaan op de blacklist te zetten, tenzij iemand betaalt voor wifi, dan wordt het MAC-adres verwijdert. Leg uit waarom dit idee van de hotel eigenaar niet mogelijk is.
38. Verzin zelf een systeem voor tijdelijke toegang tot wifi. Zorg dat je niet vatbaar bent voor spoofen en leg uit waarom jouw manier niet gehackt kan worden. Leg je idee voor aan een klasgenoot en kijk of je klasgenoot je systeem kan hacken.

Opdracht 16. De fysieke beveiliging van een access-point.

Een hacker kan natuurlijk ook proberen fysiek toegang te krijgen tot WAP en dan bijvoorbeeld met een kabel haar laptop verbinden met het netwerk. Het is belangrijk om de access points daarom goed te beveiligen. Bij het inrichten van gebouwen wordt daar zelfs rekening mee gehouden. De volgende vragen gaan over de locatie van de wifi router.

39. Ga op onderzoek in je school, zoek wifi access points en bekijk of het mogelijk zou zijn voor hacker om met een netwerkkabel toegang te krijgen tot het netwerk (niet echt doen, dat is illegaal!).
40. Noem een locatie waarbij het een stuk moeilijker zou moeten zijn om een netwerk kabel in te steken, leg uit waarom
41. In Figuur 1.10 zie je een afbeelding van een kantoor, zie jij waar de WAP hangt? Is dat een makkelijke plek voor een hacker? Leg uit.
42. Waar staat je wifi-router thuis? Hoe moeilijk is het daar?

FIGUUR 1.10 KANTOOR MET WAP

6. Versleuteling bij wifi-netwerken

Om indringers tegen te houden kun je natuurlijk het wifi-netwerk beveiligen met een wachtwoord. Daarnaast is het belangrijk om de berichten die worden uitgewisseld tussen apparaat en WAP zijn versleuteld. Daar gaan we in dit hoofdstuk op in.

Er zijn drie protocollen voor versleutelingen die momenteel worden gebruikt voor de beveiliging van wifi-netwerken: WEP, WPA en WPA2.

Voordat je verder gaat is het belangrijk om een verschil te maken tussen:

- het wachtwoord voor toegang tot de configuratie van de WAP of wifi-router;
- de netwerksleutel: het wachtwoord dat nodig is om te verbinden met het wifi-netwerk.

In dit deel gaat het over de netwerksleutel. WEP, WPA en WPA2 maken gebruik van deze netwerksleutel. Het is vaak een groot deel van het geheim van de persoonlijke sleutel. Daarom wordt het ook als een groot probleem gezien als mensen open en bloot vertellen over hun netwerk sleutel. Denk maar eens aan een restaurant die het op de menu kaart heeft staan of een koffie tent die een bord aan de muur heeft hangen zoals in Figuur 1.10

We gaan ze een voor een onder de loep nemen.

FIGUUR 1.11 NETWERKSLEUTEL

WEP

Wired Equivalent Privacy, ook wel **WEP** genoemd is de eerste versie van versleuteling die werd gebruikt voor de berichten van een router. WEP kwam als eerste versleuteling techniek met het 802.11 protocol uit in 1997. Ondanks dat het al een tijd geleden is, zijn er nog steeds 32.5 miljoen wifi routers wereldwijd die momenteel deze encryptie gebruiken. Wat eigenlijk wel bijzonder is want sinds 2004 is het als ouderwets verklaard.

Er wordt in de praktijk over twee varianten van WEP gesproken. Namelijk **WEP open** en **WEP gedeeld**. Bij *WEP open* wordt de sleutel voor vercijfering van de gegevens door de WAP naar het apparaat verzonden. Het WAP en het apparaat gebruiken dezelfde sleutel. Bij WEP open gebruikt de WAP maar één sleutel voor alle apparaten.

Opdracht 17. Aanval op WEP open

43. Wat kan een hacker doen om berichten te lezen die worden versleuteld door WEP open.
44. Is WEP open veilig?

WEP gedeeld is de WEP waar je vaker mee te maken krijgt in de praktijk als je WEP gebruikt. Hierbij wordt de sleutel waarmee alles wordt versleuteld niet zomaar verstuurd. Het versturen van deze sleutel bestaat uit 4 stappen.

1. Het apparaat stuurt een authenticatie request naar de WAP (Zie Figuur 1.4 bericht 3)
2. Dat WAP stuurt een stuk tekst het apparaat zonder versleuteling. Deze tekst is elke keer anders.
3. Het apparaat gebruikt dan een combinatie van een netwerksleutel (ingevuld door de gebruiker tijdens verbinding maken met lengte van 40 bits) en een willekeurig nummer van 24 bits om een sleutel. Deze gecreëerde sleutel wordt gebruikt om dit stuk tekst te versleutelen. Het apparaat stuurt het willekeurige nummer van 24 en het versleutelde bericht dan naar de WAP.
4. De WAP creëert de sleutel op basis van de netwerksleutel en het willekeurige nummer van 24 bits. De WAP ontcijfert het ontvangen bericht en controleert of dit hetzelfde is als het verstuurde bericht in stap 2. Als dat geval is stuurt de WAP een bevestiging en volgt de rest van het 802.11 protocol. De data wordt steeds vervolgens versleuteld verstuurd.

De geheime sleutel wordt nooit open en bloot verstuurd, waardoor het veiliger is dan WEP open. De geheime sleutel om daarna berichten te versturen is dus de netwerk sleutel gecombineerd met het willekeurige nummer. In het protocol wordt niet benoemd dat het willekeurige nummer steeds moet veranderen. De meeste apparaten werken constant met dezelfde geheime sleutel.

Opdracht 18. Aanval op WEP gedeeld

45. In hoeverre is WEP gedeeld veilig in jouw ogen?
46. Wat zou je moeten verbeteren om hiervoor minder kwetsbaar te zijn?

Je zult er misschien niet verbaast van staan, maar WEP werd al gebroken in 2001 door middel van brute force attack. Toen was de hardware nog niet heel snel waardoor dit wel 10 uur duurde. De FBI brak daarna *WEP gedeeld* in 2005 in 2 minuten. Daarom werd er afgestapt van WEP en kwam de Wifi Alliance met WPA. Voor WPA en WPA2 wordt het 802.11i protocol gebruikt wat is afgeleid van het 802.1x protocol. In de praktijk ziet dit hetzelfde eruit als het 802.11 protocol. Alleen zijn er extra stappen toegevoegd tussen bericht 4 en 5 (zie Figuur 1.4). In die stappen wordt een gezamenlijke sleutel uitgewisseld. Bij WEP zagen dat deze sleutel voor versleuteling gelijk was aan de netwerksleutel plus een willekeurig nummer. Bij WPA en WPA2 is dat wat complexer.

WPA

Nadat WEP in 2001 al gebroken bleek, was het zaak voor de Wifi Alliance om met wat beters te komen. Als tussentijdse oplossing kwamen ze met *Wi-Fi Protected Access*, ook wel **WPA** genoemd. In april 2003 werd deze standaard encryptiemethode uitgerold en op het moment gebruiken nog 30 miljoen wifi-routers WPA.

Bij WPA worden de sleutel of het willekeurige getal niet leesbaar verzonden. Daarnaast zijn de sleutels langer. De sleutellengte is namelijk 256 bits en het willekeurige nummer is 48 bits ipv 24 bits.

Het doel van WPA is dat elke apparaat een unieke sleutel gebruikt, alhoewel WPA vaak gebruikt wordt in pre-sharedkey mode (PSK), hierbij gebruiken alle gebruikers dezelfde sleutel zoals we al eerder zagen in WEP. WPA maakt ook gebruik van *Temporal Key integrity Protocol* (TKIP). Dit is een mechanisme dat een kleine subsleutel maakt op basis van de netwerksleutel. Eens in de zoveel tijd wordt een nieuwe subsleutel gemaakt en dus een nieuwe sleutel voor vercijfering van de berichten.

Desondanks bleek al gauw dat ook WPA niet veilig is. De reden hiervoor was dat de transitie van WEP naar WPA snel was gegaan, dus werd er vaak nog gebruikt gemaakt van hardware die origineel was ontworpen voor WEP. Men zegt ook wel dat het spook van WEP nog altijd actief was bij WPA. Het resultaat was dat ook WPA snel werd gekraakt en dat de Wifi Alliance een nieuwe versie uitbracht: WPA2.

Opdracht 19. WPA en zijn zwakheden

47. Leg uit waarom WPA veiliger werd door de sleutel lengtes groter te maken?
48. Geef een voordeel van TKIP ten opzichte van PSK.

WPA2

Het was 2006 toen de Wifi Alliance officieel begon met het uitbrengen van **WPA2**, de derde versleutelingsmethode in nog geen 10 jaar tijd. Op dit moment gebruiken ongeveer 430 miljoen wifi-routers deze methode. Een belangrijke verbetering is dat gebruik wordt gemaakt van advanced encryption standard (AES), op het moment een van de sterke encryptiemethoden. Tot nu toe is WPA2 de veiligste methode. De sleutel van WPA-2 is, net zoals bij WPA, ook 256 bits lang.

Toch is het gelukt om een aantal succesvolle aanvallen uit te voeren op WPA2. In 2017 kwam de zogenoemde KRACK attack (zie: https://www.krackattacks.com/). Er wordt daarbij slim gebruik gemaakt van een zwakheid. Het is namelijk mogelijk om met bepaalde berichten de wifi-router een al gebruikte sleutel te laten gebruiken. De conclusie is dat WPA2 ook aan vervanging toe is, er wordt gewerkt aan WPA3.

De conclusie van dit verhaal is dat de Wifi Alliance veel bezig is geweest met het vinden van een veilige versleutelingsmethode. WPA2 is de meest gebruikte op dit moment, maar ook deze methode heeft zijn zwakheden.

Opdracht 20. KRACK ATTACK

Het volgende artikel https://www.security.nl/posting/535615/KRACK-aanval+op+WPA2-beveiliging+wifi-netwerken%3A+Een+Q%26A gaat over de KRACK attack op WPA2.

Lees het artikel en beantwoord dan de volgende vragen:

49. Welke besturing systemen zijn voornamelijk kwetsbaar volgens het artikel?
50. Wat kan een aanvaller doen met behulp van de KRACK-?
51. Wat kun je doen om je hiertegen te beschermen?

Opdracht 21. WEP,WPA,WPA-2, welke gebruik ik?

In deze opdracht ga je onderzoeken welke van de drie methoden jouw telefoon of computer gebruikt op jouw netwerk. Doe deze opdracht samen met een klasgenoot en vergelijk ook jullie resultaten.

52. Zoek uit welk protocol gebruikt wordt op:
    - School
    - Thuis

- Een wifi netwerk van een winkel of café

Op je telefoon kom je erachter door op het netwerk te drukken waarmee je nu verbonden bent. Druk dan op de instellingen/details van dat netwerk. Daar staat meestal het versleutelingsprotocol dat wordt gebruikt.

Op de computer, ga naar je wifi-instellingen, en druk daar op details van het wifi-netwerk waarmee je verbonden bent, daar hoort te staan welk versleutelingsprotocol wordt gebruikt.

Opdracht 22. WEP,WPA,WPA-2, link leggen

53. Verbind elk van de type netwerken met de juiste sleutellengte en beschrijving van de veiligheid. Ieder woord mag maar 1x verbonden worden.

Type netwerk	Sleutel lengte	Veiligheid
Gesloten netwerk met WEP	Geen	Niet veilig
Gesloten netwerk met WPA	64 bits	Beetje veilig
Gesloten netwerk met WPA-2	256 bits	Redelijk veilig
Open netwerk zonder versleuteling	256 bits	Beste beveiliging

Opdracht 23. Wifi-router configureren

In deze opdracht ga je een wifi-router configureren. Om een router in te stellen zul je eerst een router moeten hebben. Je zou een oude kunnen kopen bij een tweedehandswinkel, of je router thuis gebruiken. Zorg dat je wel eigenaar bent van de router.

- SSID van het netwerk
- Kanaal van het netwerk
- Het wachtwoord voor toegang tot de wifi-router
- De netwerksleutel
- De versleutelingsmethode die wordt gebruikt (WEP/WPA/WPA2)
- Zet WPS uit (zie Extra: Wifi Protected Setup (WPS))
- Mac-adresfilter instellen

54. Stel de onderstaande zaken in. In Extra: Wifi router configureren wordt dat verder toegelicht. Maar je mag ook proberen het zelf uit te zoeken. Maak steeds een schermafdruk van je instellingen.

7. Extra: Wifi Protected Setup (WPS)

Sinds 2006 wordt een WAP of wifi-router soms ook uitgerust met **WPS**. Misschien het meest onbekende, maar ook het meest kwetsbare gedeelte van de router. WPS staat voor Wifi Protected Setup en is een extra toevoeging om eenvoudig te kunnen verbinden met een wifi-router.

FIGUUR 1.12

De grootste fouten zijn er sinds 2013 uitgehaald en als je nu een wifi-router hebt vanaf 2013 zul je meestal ook wel goed zitten. WPS was een techniek, die ook een eigen logo kreeg zie Figuur 1.16, en was vooral bedoeld voor randapparatuur. Dit gaf een wifi-router onder andere een fysieke knop (zie Figuur 1.14) waarmee de router in WPS modus kwam om verbinding te maken. Een ander apparaat dat ook in WPS modus stond zou dan automatisch verbinden met de router. Op deze manier was het niet nodig om lange wachtwoorden in te typen. Met name voor IoT-apparaten (bijvoorbeeld een wekker met wifi) zou dit makkelijk zijn.

Zoals eerder gezegd had WPS ook een aantal minder goede dingen vanuit een beveiliging perspectief. Ten eerste gaf dit weer een open deur voor hackers, je hoefde nu niet per se een netwerksleutel te hebben om toegang te krijgen tot het netwerk, je kon nu gewoon toegang krijgen door op deze WPS knop te drukken.

FIGUUR 1.13 WPS-KNOP OP DE WIFI-ROUTER

Je kon apparaten aanmelden doormiddel van een 8-cijferige pincode. De moeilijke netwerk sleutel die jij had ingesteld werd helemaal buitenspel gezet hierdoor. Een 8-cijferige code zou betekenen dat je 10^8 (100 miljoen) mogelijke combinaties had om te proberen voordat je binnen kon komen. Met een brute force attack een koud kunstje ook al duurt het wel eventjes.

Er zit nog een maar aan dit verhaal, het laatste cijfer van de pincode is een controlecijfer afhankelijk van de eerste 7. Het 8ste cijfer hoef je dus niet te raden maar kan je berekenen op basis van de andere. Dat maakt het probleem al gelijk aan 10^7 = 10 miljoen mogelijkheden, een stuk kleiner dan eerst.

Maar het was zelfs nog eenvoudiger. De wifi-router liet namelijk weten als de eerste vier cijfers van de pincode correct waren.

Opdracht 24. WPS mogelijkheden

Bereken nu hoeveel mogelijkheden er over blijven door de volgende stappen te doorlopen.

55. Als eerste wil je de eerste 4 cijfers goed hebben, de mogelijke cijfers die je kan invullen lopen van 0 t/m 9. Wat is het aantal mogelijkheden?
56. Eenmaal de eerste 4 gevonden, ga je de 3 opvolgende proberen. De laatste hoeven we namelijk niet te gokken want dat is een berekening van de voorgaande 7. Hoeveel mogelijkheden zijn dat?
57. Wat is dus het totaal aantal mogelijkheden dat je moet gokken voor de juiste code (in het slechtste geval)?.

Deze aanval was door middel van gratis beschikbare software erg makkelijk uit te voeren. Als er eenmaal verbinding is met het netwerk, dan kan je ook de netwerk sleutel verkrijgen. Zie Figuur 1.16, waarbij een programma genaamd Reaver hier in 2 uur achter de code en de rest komt.

Dit was natuurlijk een groot probleem voor de beveiliging van wifi-routers, gelukkig hebben veel internet providers die routers leveren er wat aan gedaan. Een aantal fabrikanten hebben een timeout toegevoegd. Of te wel, als jij 3 keer fout hebt geraden moet jij een half uur wachten voordat je het weer mag proberen. Dit vertraagt de aanval aanzienlijk maar maakt het niet onmogelijk. Andere fabrikanten van routers zetten standaard WPS uit als je de router krijgt.

FIGUUR 1.14 REAVER

8. Extra: Wifi router configureren

In dit deel ga je leren hoe je een wifi-router moet instellen en wat je allemaal tegenkomt tijdens het instellen van een wifi router. Veel van de dingen die je tegenkomst zijn eerder al behandeld. Het draait er bij deze opdracht om dat we onze router zo instellen dat het voor een hacker erg moeilijk wordt om een aanval op de router uit te voeren. Of een aanval op de mensen die verbonden zijn met de router.

In deze paragraaf gaan we stapsgewijs onderzoeken wat je allemaal tegenkomt en moet doen tijdens het instellen van een router. Nu gebruiken we hier het voorbeeld van een Ziggo router, en daarmee zijn ook de afbeeldingen hier van een Ziggo router. Het kan dus zijn als je dit zelf doet dat het allemaal net op een andere plek staat of bepaalde dingen anders heten. In de grote lijnen draait het hetzelfde idee en je zult ook zeker dezelfde begrippen tegenkomen.

Stap 1: Inloggen op de router

Om verbinding te maken met een wifi-router is het het makkelijkst als je verbonden bent met de router via een computer met kabel. Maar zorg er vooral voor dat je verbonden bent met de router. Ga dan in de browser naar het lokale IP adres waar je router op beschikbaar is. Daar kom je als volgt achter:

Ga naar je beschikbare netwerken, druk op eigenschappen van het netwerk waar je nu meer verbonden bent.

Hier staat achter default gateway het lokale adres waar je router op beschikbaar is. Typ dit IP adres in bij je browser. In dit geval was het 192.168.178.1, waarna de router je automatisch doorstuurt naar de inlog pagina. Zie Figuur 1.17. Je kunt zien dat dit IP adres hetzelfde is als het Server IP adres dat je bij de vorige opgave bij vraag 5 als antwoord hebt gegeven.

FIGUUR 1.15 INLOGSCHERM WIFI-ROUTER

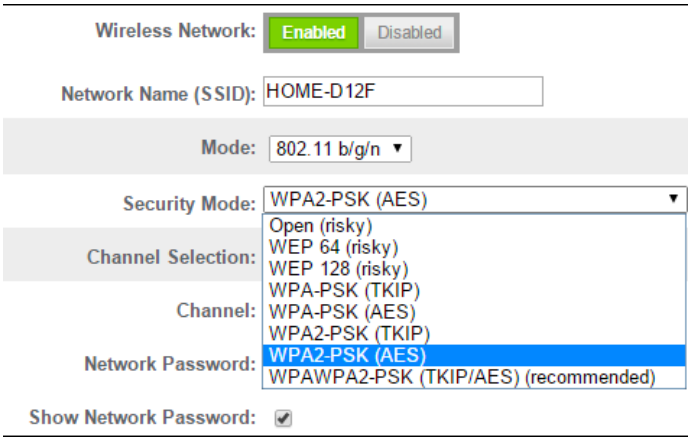
Eenmaal op de inlog pagina dien jij het wachtwoord in te vullen die is ingesteld. Let op! Dit is dus niet de netwerk sleutel. Vaak staat dit wachtwoord geschreven op de wifi router zelf(onderkant) of op een apart kaartje bijgeleverd. Mocht je het niet weten zou je nog via een kabel kunnen verbinden met je router. Mocht het wachtwoord ooit zijn aangepast en weet je het nieuwe niet meer maar heb je het oude wachtwoord nog wel, dan kan je de router een reset geven, dan wordt alles terug gezet naar de fabrieksinstellingen. Daarmee ook het wachtwoord naar wat het was toen de router werd geleverd. Dit doe je door een klein knopje 10 seconde in te drukken met een potlood of iets dergelijks. Controleer van tevoren wel even met je ouders hoe en wat, alle instellingen gaan namelijk terug naar fabrieksinstellingen. Gelukkig kan je de rest van deze paragraaf gebruiken om alles weer naar normaal te krijgen.

Stap 2: Beveiliging wifi netwerken

Ga naar de beveiliging van jouw wifi netwerken. In dit geval staat het onder Draadloos en daarna beveiliging. Hier kan je onder andere de SSID, beveiliging en de netwerk sleutel van je wifi router zien, zie Figuur 1.18. Voor SSID mag je zelf een naam kiezen die je leuk lijkt.

FIGUUR 1.16

Hier is het belangrijk dat we de beste beveiliging kiezen. Je ziet in de afbeelding dat alle versleuteling technieken gebruiken maken van PSK. Dat is erg jammer want we zagen eerder dat PSK niet een ideaal protocol is om te gebruiken. Helaas is dit wel de standaard als het gaat om persoonlijke routers. Het gevaar van persoonlijk netwerk is te laag en als je een dure bedrijf router koopt heb je vaak andere mogelijkheden. De enige reden waarom het dan nog een beetje veilig is, is omdat er gebruikt wordt gemaakt van TIKIP. Dan wordt er tenminste iedere keer een deel van de sleutel vernieuwd. In Figuur 1.19 zie je een afbeelding van een andere router die alle opties neerzet. Ondanks dat de afbeelding aanraadt de meeste onderste versie te gebruiken, is de een na laats optie toch het meest veiligst. De reden is dat bij de laatste variant ook oude apparaten kunnen verbinden die nog niet kunnen werken met WPA2. Nu is de vraag, kies je voor maximale beveiliging en daarmee WPA2-PSK met AES of wil je ook oude apparaten ondersteunen(d.m.v. WPA-PSK met TKIP) en daarmee een lek open houden in je wifi router?



FIGUUR 1.17

- Stel de juiste beveiliging in en maak hiervan een foto/screenshot

Als laatste, en hier verborgen is het belangrijk dat je een sterk netwerk wachtwoord kiest. In dit hoofdstuk is daar geen aandacht aanbesteed, maar eerder in hoofdstuk 1 kwam dit wel terug. Zorg dat je een lang en complex wachtwoord kiest wat je goed kan onthouden.

Stap 3: WPS van Wifi Router

WPS kwam ook al eerder terug in dit hoofdstuk, we zagen daar dat het lek was als een mandje en dat je voornamelijk beschermd bent als er een time out is als mensen vaker een verkeerde pin code invoerde. De beste beveiliging die een producent van een router levert is door deze pin code standaard uit te zetten. Als de wifi router op een makkelijk bereikbare plek hangt is het ook slim om de functionaliteit van de WPS knop uit te zetten. Ga via de instellingen naar de WPS instellingen. Daarna zul je iets tegenkomen dat er ongeveer uitziet als Figuur 1.20.

FIGUUR 1.18

Hier zie je dat de WPS pincode alvast uitstaat, dat is dus door de producent van de router standaard ingesteld. De WPS knop staat nog wel ingeschakeld, de keuze daarvoor mag je zelf maken. Je zou hem ook uit kunnen zetten en indien nodig zelf door middel van inloggen op de router weer aan

kunnen zetten. In de router die wordt gebruikt is het niet mogelijk om te zien of er een time out ingesteld is bij een aantal onjuiste pogingen. Zeker daarom laat ik de WPS pincode uit staan

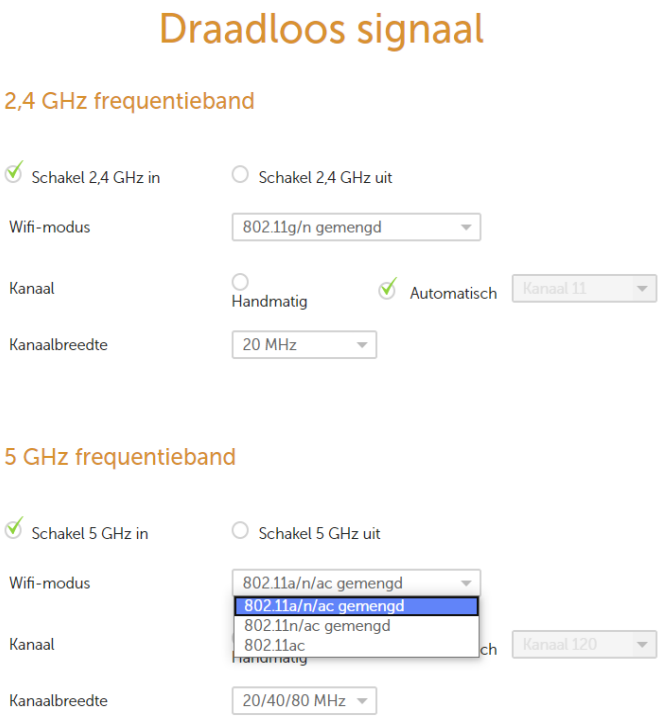
- Stel je WPS instellingen zo in dat de beste beveiliging mogelijk is. Maak een foto/screenshot van deze instellingen

Stap 4: Modulatie techniek

Ga via instellingen naar draadloze netwerken. Je zult iets in de trend moeten krijgen als Figuur 1.21. Hier kun je de verschillende netwerken aan en uitzetten. Het wordt je aangeraden om beide netwerken te gebruiken. Omdat ze over verschillende eigenschappen beschikken.

- Waarom kan je in de figuur bij 5Ghz niet de wifi modulatie g of n gebruiken die je wel ziet staan bij 2.4 GHz?

Met nieuwere modulatie technieken is er niet per se betere versleuteling gekomen. Het maakt dus vanuit een beveiliging perspectief niet heel veel uit welke techniek je kiest. Kies je de nieuwste variant, dan zul je het snelste internet hebben, maar dan heb je ook de kans dat oude apparaten geen verbinding kunnen maken. Het is daarom aangeraden om zo een divers mogelijke optie te kiezen.



FIGUUR 1.19

Eerder in Opdracht **Error! Bookmark not defined.** kon je zien op welke kanalen je wifi netwerk uitzond. Die kanalen komen hier terug en staan ingesteld op automatisch. Een wifi netwerk zit op een bepaald kanaal, en deelt daarmee vaak dat kanaal met wifi netwerken in de buurt. Indien je wifi router geen automatisch kanaal aanbiedt, zorg dan dat je deze handmatig instelt op een kanaal waar geen andere wifi netwerken zitten. Op deze

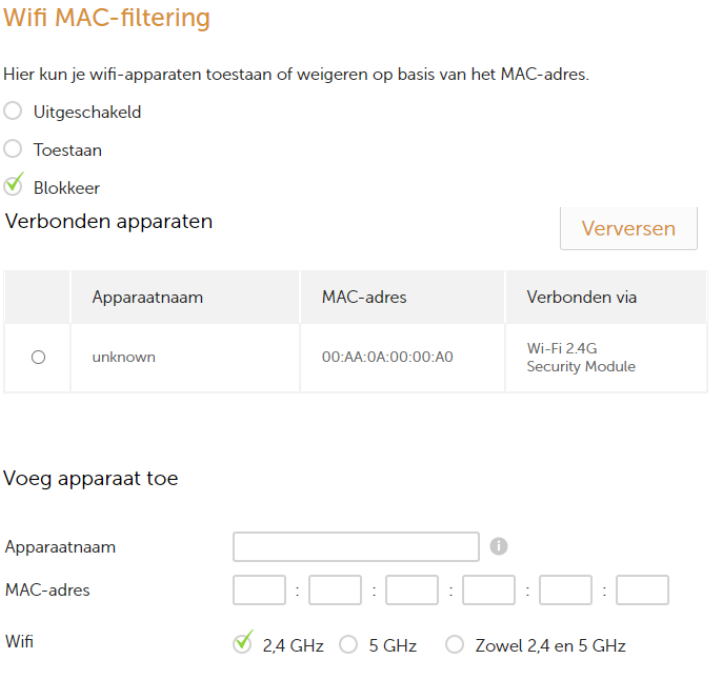
manier heeft je eigen wifi het minst last van andere netwerken en zul je een stabieler netwerk hebben. De nieuwere routers hebben een mogelijkheid waarin die automatisch opzoek gaat naar een “rustig” kanaal.

- Stel je router in op het meest rustige kanaal en controleer of dit klopt door middel van de app wifi analyzer. Maak een foto als bewijs
- Stel de wifi modulatie in naar keuze, maak een foto als bewijs dat het gelukt is.

Stap 5: MAC Filter

Als laatste gaan we kijken naar de MAC filter die je router heeft. In dit voorbeeld staat die onder beveiliging en daarna MAC-Filtering. Het scherm dat je daarna krijgt ziet er uit zoals Figuur 1.22. Je ziet hier de mogelijkheid om een lijst bij te houden met MAC adressen die mogen verbinden de zogenoemde White list of een lijst met MAC adressen die je wilt blokkeren, de zogenoemde black list. Je kunt hier eenvoudig de verbonden apparaten zien met bijbehorende MAC adressen.

- Zie jij welk apparaat van jou is? Zo ja welke? Klopt het MAC adres met het adres van het huidige apparaat?(dit heb je eerder gevonden in dit hoofdstuk)
- Kan je alle andere verbonden apparaten verklaren? Apparaten van je familie, IPad maar ook andere IOT apparaten staan er tussen. Maak een lijst met alle verbonden apparaten en schrijf erachter wat voor apparaat dit is.



FIGUUR 1.20

Het resultaat van deze paragraaf is dat je een aantal foto’s hebt gemaakt van de verschillende instellingen die je hebt gedaan op je wifi router. Laat de foto’s zien aan je docent als bewijs van deze opdracht. Als je klaar bent sla dan alles op en controleer met de app Wifi analyzer of alles klopt zoals jij hebt ingesteld.